SAIC
An Employee-Owned Company

INFORMATION PROTECTION ENGINEERING:
Using Technology and Experience to Protect Assets

William J. Marlow

Corporate Business Development
Technology Services Group

Science Applications International Corporation
1710 Goodridge Drive
McLean, VA 22102
Tel: 703/749-8679
E-mail: william_marlow@cpqm.saic.com

ABSTRACT

All businesses and government agencies are dependent on information and the systems that communicate and store this information. SAIC's highly experienced team has developed technology, techniques and expertise in protecting these information assets from electronic attack by criminals, terrorists, hackers or nation states.

Form SF298 Citation Data

Report Date *("DD MON YYYY")* 00000000	**Report Type** N/A	**Dates Covered (from... to)** *("DD MON YYYY")*

Title and Subtitle Information Protection Engineering: Using Technology and Experience to Protect Assets	**Contract or Grant Number**
	Program Element Number
Authors Marlow, William J.	**Project Number**
	Task Number
	Work Unit Number
Performing Organization Name(s) and Address(es) Science Applications International Corporation 1710 Goodridge Drive McLean, VA 22102	**Performing Organization Number(s)**
Sponsoring/Monitoring Agency Name(s) and Address(es)	**Monitoring Agency Acronym**
	Monitoring Agency Report Number(s)
Distribution/Availability Statement Approved for public release, distribution unlimited	
Supplementary Notes	
Abstract All businesses and government agencies are dependent on information and the systems that communicate and store this information. SAICs highly experienced team has developed technology, techniques and expertise in protecting these information assets from electronic attack by criminals, terrorists, hackers or nation states.	
Subject Terms	
Document Classification unclassified	**Classification of SF298** unclassified
Classification of Abstract unclassified	**Limitation of Abstract** unlimited
Number of Pages 8	

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)

2. REPORT DATE

3. REPORT TYPE AND DATES COVERED
White Paper

4. TITLE AND SUBTITLE
Information Protection Engineering: Using Technology And Experience
To Protect Asset

5. FUNDING NUMBERS

6. AUTHOR(S)
William J. Marlow

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

IATAC
Information Assurance Technology Analysis Center
3190 Fairview Park Drive
Falls Church VA 22042

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Defense Technical Information Center
DTIC-IA
8725 John J. Kingman Rd, Suite 944
Ft. Belvoir, VA 22060

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT

12b. DISTRIBUTION CODE
A

13. ABSTRACT ***(Maximum 200 Words)***

All businesses and government agencies are dependent on information and the systems that communicate and store this information. SAIC’s highly experienced team has developed technology, techniques and expertise in protecting these information assets from electronic attack by criminals, terrorists, hackers or nation states.

14. SUBJECT TERMS
Information Protection, Information Security, hackers

15. NUMBER OF PAGES

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT
Unclassified

18. SECURITY CLASSIFICATION OF THIS PAGE
UNCLASSIFIED

19. SECURITY CLASSIFICATION OF ABSTRACT
UNCLASSIFIED

20. LIMITATION OF ABSTRACT
None

INFORMATION PROTECTION ENGINEERING: USING TECHNOLOGY AND EXPERIENCE TO PROTECT ASSETS

INTRODUCTION

Science Applications International Corporation is a world leader in the development and implementation of secure systems for creating, processing, storing, and communicating information. There have been massive technology advances in the last 2 to 4 years that businesses have benefited from, but so too has the criminal faction. This technology is being used to steal money and information, and hold companies hostage. Preventing the problem or reacting to it is not an easy task when working in cyberspace. As organizations seek to increase productivity by taking advantage of state-of-the-art computing and tele-communications technology, they find themselves increasingly vulnerable to compromises of hard-won intellectual capital, business secrets, and proprietary information.

Moreover, the need to protect the integrity of information is equally important, even when confidentiality is not an issue. Data that cannot be trusted is worse than useless since it costs money and time to create and store, but provides no benefit. Even a data base that is only slightly tainted may require extensive resources to correct and validate, if it is possible to recover at all. Similarly, information which is not available when required is of no use, even if its confidentiality is secure and its integrity intact. SAIC has created security engineering processes to ensure that valuable information assets and data systems are protected, that intrusions from without and abuses by insiders are detected, and that effective corrective action can be taken should problems arise.

THE THREAT

The scope of the challenge organizations face can not be understated. All businesses and government agencies around the world are dependent upon the information storage and communications capabilities of their supporting systems. Newspapers, magazines, television, movies and even comic books glamorize and herald the “hacking” of computers and communications systems. The governments of the world have coined the term “information warfare”; The hackers call themselves “cyberpunks”; and organized crime, drug cartels and criminals call it “opportunity”.

As an example of the dangers inherent in networked systems, consider that during the past year illicit password collection devices called “sniffers” have been and continue to be installed in ways that allowed the theft of user passwords from major Internet service providers in the United States and other countries. Using these compromised passwords, intruders have gained unauthorized access to computers in academic and government institutions and a variety of commercial enterprises. In some cases these hackers were able to take over the control of computers, read and steal files, install “back doors” and Trojan Horses to ease reentry, and examine software under development. In some cases, they even destroyed files.

Both government and commercial firms have experienced these attacks, which resulted in massive theft and computer fraud, and caused hundreds of millions of dollars or more in lost revenues and costs to repair systems and replace data. Credit-card fraud based on improper authentication of card users has cost the world-wide economy billions, and both the telephone-service providers and commercial entities operating their own PBX and voice-mail systems have been hit with massive toll fraud.

These challenges must be met in the context of a highly dynamic information environment. The global Internet web is enjoying a double-digit compound annual growth rate with predictions of a billion users by the turn of the century1. Already, untold numbers of individuals have direct access to these computers or indirect access via local area networks. Government organizations and commercial enterprises are rapidly becoming interconnected via networks (such as the Internet) in order to enable or improve the efficiency of transactions. Unless special precautions are taken, these same pathways become, unfortunately, the doors through which the criminal or industrial spy intent on theft of money or intellectual property, or on simply causing damage, enters the enterprise’s information systems.

SAIC approaches security engineering with the understanding that information has an associated value to either criminals or nation-states. There may be a liability that translates into economic loss for the holder of information, if information is lost or compromised. This may be due either to the loss of direct value resulting from the loss of information, process, or privacy, or to the loss of indirect value from a judgment for breech of trust because due diligence was not exercised in protecting the confidentiality, integrity, or availability of the data.

If data is valued for its scarcity, access to the information must be restricted. Some information is subject to attorney-client or doctor-patient privilege, and other information may be held in trust for clients, customers, vendors, or employees. In the national security environment the degree of required protection is spelled out in rules and procedures for “classified” and for “sensitive but unclassified” information. In the commercial sector similar actions to limit access must be undertaken to protect the commercial advantage contained within intellectual capital, trade secrets, or other proprietary information.

Newspaper headlines tell the story:

- *USA Toda*y, 5/23/96, Front Page
  Headlines “Pentagon Reports
  250,000 Hacker Penetrations”
- Citibank announced 5/12/95
  they had been hacked by a Russian
  for up to $10M
- California Banks defrauded of $50M
- London Banks defrauded of $460K
- Fiji Bank defrauded of $2M.

And so on. It is international, it is potent, and it is a solvable problem.

SECURITY ENGINEERING ANDTECHNOLOGY

Information protection is a risk management problem for businesses and governments alike: how much needs to be spent to protect what information, against what is an acceptable loss.

Managing the risk posed to information assets requires, in addition to awareness of the threats faced, an appreciation for the vulnerabilities inherent in available data processing and telecommunications systems, and knowledge of the technologies, practices, and procedures that can be employed for protection; detection of intrusions, abuses, and computer misuse: and correction of problems. These factors must be considered within the context of how valuable the information is, and what losses might be sustained were it to be compromised, misused, or destroyed — versus the costs of implementing protective countermeasures. The risk management decisions that must be made are shaped by corporate policy and procedures, and the systems engineering process; in short Information Protection is the result of security engineering.

Information can be considered as existing in one of four states:

- It is being created (as at a point-of-sale or an authoring or design activity),
- It is being transferred from one location to another,
- It is being manipulated via some transaction in order to enable some business or functional process outcome, or
- It is being stored at rest as an archive or data base for future use.

The protection of information value requires an examination of risk of accidental or intentional damage or loss in each of these states.

The information in these states fall into 2 categories — either requiring protection or under attack. In the latter case time is of the essence, since the longer an intruder has access, the more doors that person(s) can put in to prevent you from stopping them.

The first step is to identify the path of access. The most common methods to identify access paths are to install network sniffers (devices that read all information on a network), or to employ X.25 communication lines or Frame Relay technology. A network sniffer bypasses any computer program and reads the raw data. In this way every keystroke can be monitored and captured for analysis.

The problem with networks is that information arrives in mix packets belonging to multiple sessions. In a common banking data center this is about 200 concurrent sessions. Special software needs to be available which will reassemble the packets in the right order so they are readable. The software with most sniffers is too slow to accomplish this and to display/record to high-speed devices in real time.

SAIC has designed software written in Peral Script and C++ which will in real time read, record, and assemble up to 20,000 packets an hour representing approximately 500 concurrent sessions per communications line. This allows the direct viewing and analysis of on-going traffic to identify the primary pathway. This becomes critical when the pathway is a Frame Relay in which the header packets direct the flow of information, or where a SONET (Fiber Optic) net is used. **Figure 1** represents a typical network implementation where intruders have multiple unprotected high speed access points. This speed adds another level of complexity-analysis. Being able to record the data is no trivial pursuit, but it is even more difficult to analyze this high amount of information.

SAIC has developed intelligent software agents to analyze this information based upon critical knowledge about the various businesses, their practices, processes and normal flow of information. These intelligent agents reduce the amount of information from the equivalent of about 10,000 pages to 50 or 60 pages of information.

Once data has been captured, the task of identifying the process used to gain access must be reverse engineered at the same time as control mechanisms are put in place to prevent the intruder from shutting down the network (this is the worst scenario for a bank, brokerage, insurance company, etc.). The control mechanisms will range from reconfiguring routers to shadow servers which will be cut in as hot transfers.

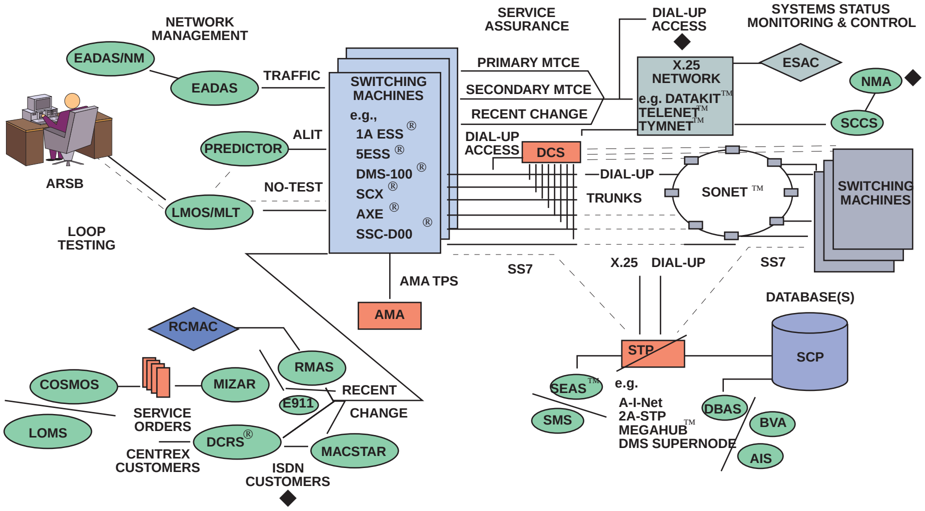

Figure 1. Typical Network Implementation and High Speed Entry Points (◆)

The reverse engineering effort is intended to determine how much information the intruder may have, and then design an approach to capture access points and terminate them with little impact on the business. **Figure 2** represents how intruders have actually assembled the diverse pieces of "innocent" data in order to develop an overall attack on a network and a client. Using a combination of good system engineering techniques and intelligence analysis processes it is possible to rebuild the mosaic of knowledge the intruders may have which will define the approach to stopping them.

A more proactive approach addresses the first category: information requiring protection. This process involves a combination of systems engineering and business analysis. We apply a variety of investigative tools which give us a unique picture of the business, its technical vulnerabilities, and possible areas of system compromise. **Figure 3** illustrates a flow of activities utilized in performing an analysis of business information/data system. Track "A" and "B" are performed concurrently, and conclude with an overall assessment/ recommendation report.

Some of the diagnostic and assessment tools SAIC utilizes are listed below. These range from vetted "hacker programs" to commercially available tools. A selection of these is provided in **Table 1**.

This systems approach summarized in **Figure 3**, allows us to find most of the potential problem areas, and helps deter some of the more sophisticated attacks that have been used. We maintain a detailed knowledge base of attack techniques. These techniques range from social engineering (the art of being a good liar) to very sophisticated penetration and deception programs. Listed below are some of the more recent ones used.

1. **Simple Methods**

- Social engineering (e.g., criminal impersonation) via
  - free upgrades
  - customer support
  - cyber friends
  - insiders

2. **Sophisticated Methods**

- Plain text encryption of programs and messages
- Multi-path/multi-part program insertion
- Graphics transfer using last bit of each pixel
- Physical compromise of nodes, routers and networks
- Spoofing of addresses
- Eavesdropping on telecommunications networks and downstream spoofing
- Modification of transmissions

We then apply a technique known as Probabilistic Risk Assessment (PRA) to quantify the risk in terms senior managers can relate to their businesses. By quantifying the risk in terms of possible loss, management can make business decisions based on the amount of acceptable risk. Once the risk is understood, a logically defined process can then be implemented.

After completing the initial analysis process shown in **Figure 3**, SAIC uses a standard process called STEPS to implement a security technology. STEPS is an acronym for Strategy to Enhance Protection Smartly and consists of the following four phases:

STEPS 1: Assess Current Environment

- Business vulnerabilities
- Configure systems for protection
- Real threats

STEPS 2: Close Exploitable Holes

- Information exchanges
- Audit reduction and alert systems
- Vendor updates
- Outside contractors
- Crisis plan
- Training

STEPS 3: 3D Architecture (Design, Document & Deploy)

- Plans and policy
- Strategic plans
- Requirements
- Architecture

STEPS 4: Strategically Deploy Technology

- Physical locations
- Unique protection
- Token-based One time passwords
- Encryption
- Digital signatures
- Firewalls
- Security administration tools
- Network view vulnerability sensors

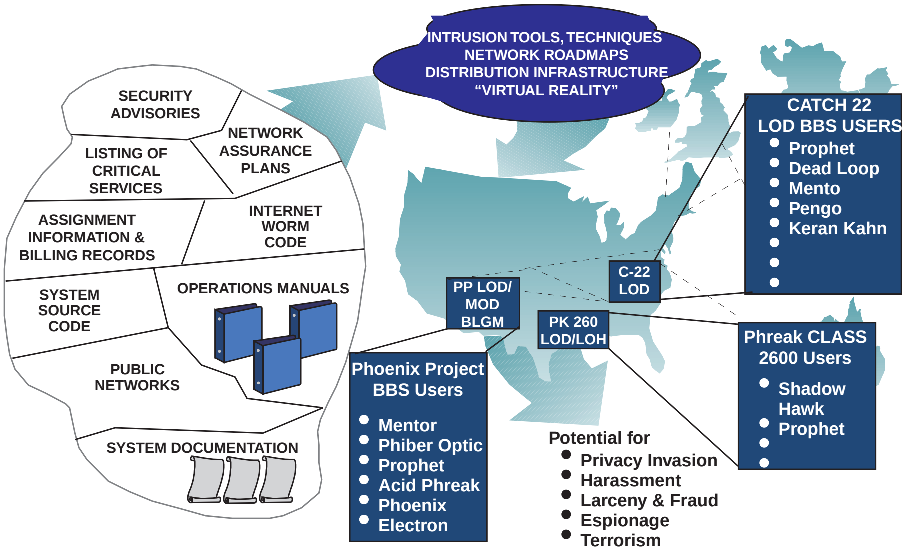

Figure 2. Mosaic Theory Applied to Intrusions

APPLICATIONS

SAIC's Information Security experts have dealt with some of the worst security problems encountered in the field to date. For one very large international bank SAIC provided crisis support when they were attacked by an organized crime group. The organized crime group penetrated the bank's systems by scanning all their available phone numbers and locating a modem that they could access. From there they entered the network, subverted the internal security, and placed "Trojan horses" (back-door entry ways) into all the key systems. Then for the next two years they slowly extracted money via these access points.

- Security Profile Inspector (SPI)
- Check Promiscuous Mode (CPM)
- Karlbridge Libldent
- Pldent
- S/Key
- SOCKS (ver 3.0 and 4.1)
- TCPR
- Janus
- ISSI
- Rampant
- UDPrelay
- Xforward
- Netman
- COPS
- IFStatus
- ISS
- TCP/Wrappers
- Traceroute
- PCAL
- LogDaemon
- TCPWho
- POrtmap
- RPCBind
- SecureLib
- Anlpasswd
- CRACK
- Npasswd
- obvious-PW
- passwd+
- Shadow
- RAIC IACS
- Swatch
- TAMU-Drawbridge
- TAMU-Netlog
- TAMU-SPAR
- TAMU-SRA
- TAMU-Tiger
- Tripwire
- Watcher
- DIG
- Fremont
- Gated
- Host
- Lsof
- NFSWatch
- Rdist
- TCPDump
- WatcherT
- SNAM
- Warrior
- Arent
- Satan
- Metaraid
- Asset
- NLook
- ISS

Table 1. Diagnostic and Assessment Tools Utilized by SAIC

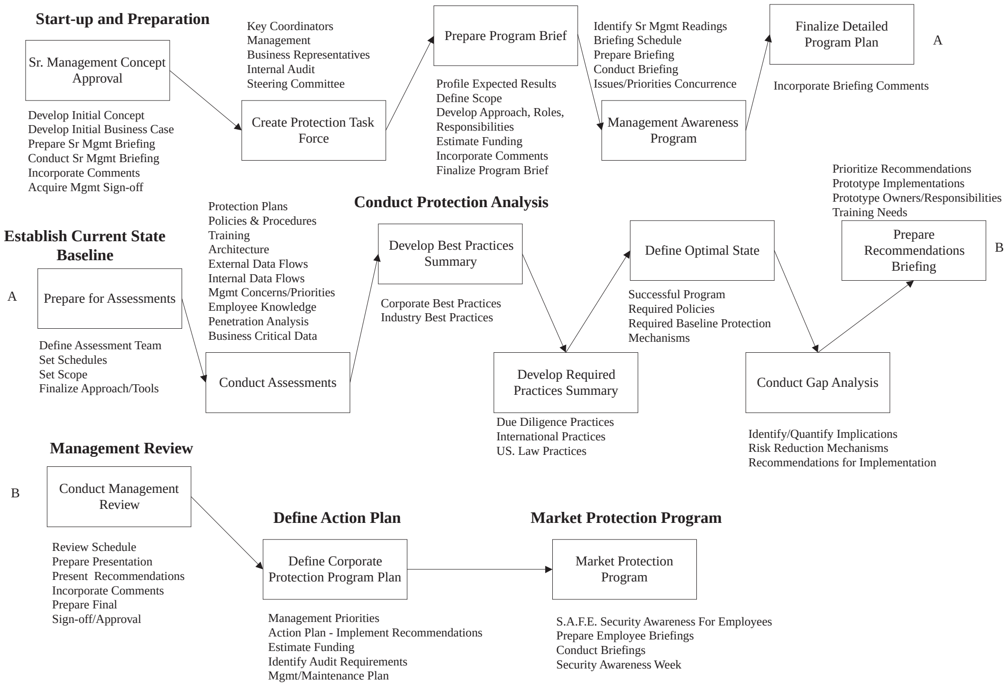

Figure 3. Generic Analysis/ Assessment Process

Unable to detect all of the entry paths or processes that were being used, the bank called SAIC's Security Emergency Reaction Center (SERC). The team immediately installed equipment to monitor and capture data to pinpoint the entry paths, scanned the systems for unusual code, and correlated the attack paths and transfers. Once the attack paths were defined, the SERC team installed software to take control of the network, and then implemented the process to stop the criminals while maintaining control over the critical portion of the networks to ensure they did not shut down the bank — a successful end to a really bad problem. Subsequently SAIC personnel designed an overall security architecture for the bank which will significantly reduce their risk and exposure.

Another example is a large conglomerate which requested a vulnerability assessment of its system. The SAIC team found an easily exploited vulnerability that allowed the generation an electronic payment via the Internet from the client's systems. Since the responsible parties believed they had sufficient security, they were very surprised and distraught that such an action was possible. Some elementary design work and implementation by SAIC corrected the problems and streamlined their process, resulting in a Return on Investment (ROI) within a year.

The Center for Information Protection (CIP)

In order to better serve our clients, SAIC created the Center for Information Protection (CIP). The purpose of the Center is to provide a repository of highly skilled individuals with world-wide, hands-on experience to our customers. The CIP can address the needs and requirements of just about every type of business. The Center coordinates various activities including monitoring of "hacker" electronic bulletin boards, research and testing of products and services, training, process/standards development, tracking of world-wide legal impacts, development of new technology, and crisis management and support.

The CIP personnel can also implement this technology in a wide variety of applications in all of the security disciplines related to protecting the confidentiality, integrity, and availability of information assets and systems. These are further described below.

Risk Assessment, Verification and Validation of Security Capabilities and Limitations

Since SAIC thoroughly understands what makes systems and networks secure or insecure, and has dealt with real-world penetrations of firms by drug cartels, organized crime, and individuals attempting to steal resources, commit fraud, and cause damage, we can assist our clients with evaluation of the security features capabilities and limitations of their systems and networks. We can perform analyses supporting risk management, including: risk analyses, assessments of threats and vulnerabilities, testing of security features and countermeasures, fraud, penetration testing, and information asset valuation. SAIC uses a formal risk analysis process and hands-on testing to determine requirements for policy, procedures, hardware and software to ensure a business-oriented balance of security and risk. The process identifies the potential for accidental or malicious misuse of computing and telecommunications assets that support the functions of the business. Finally, the risk analysis process also examines the integrity of the hardware, software, and data.

Security Systems Integration and Reengineering

We design, develop, testbed, and implement secure systems and networks, including reengineering of existing systems and networks to enhance their security features and characteristics. With few exceptions, SAIC does not produce products, so we are able to identify, without bias, the best-available state-of-the-art secure products from any source in developing or reengineering secure systems and networks for their use. These secure products are used to implement one-time passwords for access control, to add firewalls, and to incorporate auditing and audit data reduction capabilities to detect intrusions or abuses by authorized users.

Crisis Management

Our Security Emergency Reaction Center (SERC) provides both support for planning the recovery from an intrusion, and rapid emergency response to security incidents with a team of specially trained people who can quickly and accurately suppress an electronic intrusion.

Open Source Monitoring

SAIC personnel monitor the Internet, various BBS systems, electronic forums, “hacker” publications, and Freenet, for activities related to clients and their environments. By doing this, we can provide clients with the latest information about potential threats and vulnerabilities targeted toward them.

Information Protection and Security Outsourcing

Some of our clients prefer to have a trusted third party implement, monitor, and serve their security needs. We provide professional services to meet our clients’ expectations and requirements. We can assume control of the information protection/security for a customer, usually for less than the cost of creating the necessary resources internally. This provides a customer access and implementation of the full range of SAIC's information protection/security capabilities, which are always current and up-to-date.

Secure Electronic Commerce

Doing business on the Internet will become necessary for a number of businesses. There are a variety of security methods which can be applied to conduct electronic commerce. There is currently no one standard; therefore, the implementation which a firm might employ now will most likely be modified within the next several years. SAIC can help select the most extensible, compatible and protected means for the designated protection level.

Other Applications

Providing protection for information through quality security processes is a critical aspect of every system. However, the broader benefits of a well-protected system are often overlooked: better reliability, recoverability, and flow management. Since a system or business which has an active protection program will have optimized their systems and communications, the resulting changes in these factors are unique benefits that have a definable ROI.

Trends in Information Protection

In the future, information protection and security features will become a standard part of every business’s purchase of telecommunications and computer systems. Indeed, these features are already becoming the critical criteria used in designing means to bring customers and firms together for on-line transactions. Increasingly, hardware and software manufacturers are building security features into their products. Unfortunately, many of these features do not scale well when deployed in large enterprises. In addition, the interfaces between products from different vendors are often incompatible and create new security vulnerabilities. Thus, informed security engineering will remain on the critical success path for the successful protection of a firm’s information resources. The following paper by Paul Proctor provides a detailed description of a computer misuse detection system specifically developed by SAIC to address these and future needs.

References

1. *Information Week,* 7-17-95